2025/2026

Lecturer : H. MOUFEK

# Algebra 1 - Tutorial 4

Basic Training Cycle

Algebraic Structures

## Exercise 1

Let $(G, *)$ be a group with three elements. Construct its multiplication table.

## Exercise 2

Let $(E, *)$ be a set equipped with a binary operation and let $e \in E$ such that :

(a) $\forall x, y, z \in E :\ (x * y) * z = (y * z) * x$.

(b) $\forall x \in E,\ x * e = x$.

(c) $\forall x \in E,\ \exists x' \in E : x * x' = e$.

1. Prove that the operation $*$ is commutative.
2. Prove that $(E, *)$ is a commutative group.

## Exercise 3

Let $G = ]-1, 1[$. We define for all elements $x$ and $y$ of $G$ :

$$x * y = \frac{x + y}{1 + xy}.$$

1. Verify that $*$ is an associative binary operation on $G$.
2. Show that $(G, *)$ is a group. Is it commutative ?
3. Provide an expression for $x^{*n}$.

## Exercise 4

Let $(E, *)$ be a set equipped with a binary operation, associative and possessing a neutral element $e$.
Assume moreover that $\forall x \in E,\ x * x = e$.
Show that $(E, *)$ is an abelian group.

## Exercise 5

Let $G = \mathbb{R}^* \times \mathbb{R}$. For $(x, y), (x', y') \in G$, define the binary operation :

$$(x,y) * (x',y') = (xx',\ xy' + y).$$

**1** Verify that $*$ is an associative binary operation on $G$.

**2** Verify that $(G,*)$ is a group. Is it commutative?

**3** Give a closed form for $(x,y)^{*n}$.

## Exercise 6

We define on $\mathbb{R}$ the internal composition law $\star$ as follows :

$$\forall x,y \in \mathbb{R} : x \star y = x + y - 2$$

**1** Show that $(\mathbb{R},\star)$ is an abelian group.

**2** Let $n \in \mathbb{N}^*$. We define $x^{(1)} = x$ and $x^{(n+1)} = x^{(n)} \star x$.

- **a** Compute $x^{(2)}$, $x^{(3)}$, and $x^{(4)}$.
- **b** Show that $\forall n \in \mathbb{N}^* : x^{(n)} = nx - 2(n-1)$.

**3** Let $H = \{x \in \mathbb{R} : x \text{ is even}\}$. Show that $(H,\star)$ is a subgroup of $(\mathbb{R},\star)$.

## Exercise 7

Let $G$ be a group and let $H$ and $K$ be two subgroups of $G$.

**1** Prove that $H \cap K$ is a subgroup of $G$.

**2** Prove that $H \cup K$ is a subgroup of $G$ if and only if $H \subseteq K$ or $K \subseteq H$.

## Exercise 8

Let $G$ be a group. Given an element $a \in G$, define the map

$$\varphi_a : \begin{cases} G \longrightarrow G \\ x \longmapsto axa^{-1}. \end{cases}$$

**1** Let $a \in G$. Show that $\varphi_a$ is an automorphism of $G$.

**2** Define $\mathcal{I}(G) = \{\varphi_a \mid a \in G\}$. Show that the set $\mathcal{I}(G)$ is a subgroup of $(\mathrm{Aut}(G),\circ)$.

**3** Show that the map

$$\varphi : \begin{cases} G \longrightarrow \mathrm{Aut}(G) \\ a \longmapsto \varphi_a \end{cases}$$

is a group homomorphism.

## Exercise 9

Let $(G, *)$ be a group. The *center* of $G$ is the subset $C \subset G$ defined by

$$C = \{x \in G \mid \forall y \in G,\ x * y = y * x\}.$$

Show that $C$ is a subgroup of $(G, *)$.

## Exercise 10

We denote by $\mathbb{Z}[\sqrt{3}]$ the set of real numbers of the form $a + b\sqrt{3}$, where $a, b \in \mathbb{Z}$.

**1** Show that $\mathbb{Z}[\sqrt{3}]$ is a subring of $(\mathbb{R}, +, \times)$.

**2** Show that the function

$$f : \begin{cases} \mathbb{Z}^2 & \to \mathbb{Z}[\sqrt{3}] \\ (a, b) & \mapsto a + b\sqrt{3} \end{cases}$$

is a group isomorphism from $(\mathbb{Z}^2, +)$ to the group $(\mathbb{Z}[\sqrt{3}], +)$.

**3** For every $x \in \mathbb{Z}[\sqrt{3}]$, there exists a unique pair $(a, b) \in \mathbb{Z}^2$ such that $x = a + b\sqrt{3}$.

**a** For every real number $x = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ with $(a, b) \in \mathbb{Z}^2$, the conjugate of $x$, denoted $\tilde{x}$, is the real number $a - b\sqrt{3}$. Show that the function

$$g : \begin{cases} \mathbb{Z}[\sqrt{3}] & \to \mathbb{Z}[\sqrt{3}] \\ x & \mapsto \tilde{x} \end{cases}$$

is a ring automorphism.

**b** For every $x = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ with $(a, b) \in \mathbb{Z}^2$, define $N(x) = x\tilde{x}$. Verify that for all $(x, y) \in (\mathbb{Z}[\sqrt{3}])^2$, $N(xy) = N(x)N(y)$.

**c** Show that $x \in \mathbb{Z}[\sqrt{3}]$ is invertible if and only if $N(x) = 1$ or $N(x) = -1$. What is its inverse in each case ?

## Exercise 11

Let $d \in \mathbb{N}$ be such that $\sqrt{d} \notin \mathbb{Q}$. Define

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid (a, b) \in \mathbb{Q}^2\}.$$

Show that $(\mathbb{Q}(\sqrt{d}), +, \cdot)$ is a field.